METHOD AND SYSTEM FOR PERFORMING ON-LINE STATUS CHECKING OF DIGITAL CERTIFICATES

5 ABSTRACT OF THE INVENTION

A method and system for performing on-line status checking of digital certificates. Specifically, the present invention describes a communication system having a client and a server coupled together. The client requests

10 information from the server. A secure communication session is established between the client and the server for checking the revocation status of a digital certificate associated with the information. As such, further authentication of communication about the certificate status between the client

15 and the server is unnecessary. A status request pertaining to the digital certificate is sent by the client to the server. The server checks the revocation status of the digital certificate against a current digitally signed certificate revocation list. The server notifies the client

20 as to the revocation status of the digital certificate prior to any transmission of information.